PATENT ABSTRACTS OF JAPAN

(11)Publication number : **10-208388**
(43)Date of publication of application : **07.08.1998**

(51)Int.Cl. **G11B 20/10**
G09C 1/00
G11B 7/00
H04L 9/08

(21)Application number : **09-021989**
(22)Date of filing : **21.01.1997**

(71)Applicant : **VICTOR CO OF JAPAN LTD**
(72)Inventor : **MOCHIZUKI MASAKI**

(54) OPTICAL DISC CIPHER KEY GENERATING METHODCIPHER KEY RECORDING METHODCIPHER KEY RECORDING DEVICEINFORMATION REPRODUCING METHODINFORMATION REPRODUCTION PERMITTING METHODAND INFORMATION REPRODUCING DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To lower the value of information to be paid by a user and the price of a disk itselfto prevent an illegal copyand to facilitate the management of cipher key.
SOLUTION: A disk reproducing device 2 reads information characteristic of a recording medium 1 where information is recorded for discriminating the recording medium from other recording media out of the recording medium and reads out an arbitrary password code that the user of the recording medium 1 has setand a software house 3 performs arithmetic process based upon specific algorithm by using the information and password code characteristic of the recording medium 1 to generate a cipher key for reading information out of the recording medium 1. When the user wants to read the information outthe disk reproducing device 2 allows part or the whole of the information recorded on the recording medium 1 to be erased according to a password code which is inputted at this time and the cipher keywhich has been generated.

CLAIMS

[Claim(s)]
[Claim 1]The 1st field where optical recording of the information peculiar to said optical disc that an optical disc in which information was recorded is discriminated from other optical discs was carried outIt adds to information peculiar to said optical discarbitrary passwordsor theseInformation which specifies at least one of

two or more of the information currently recorded on said optical disc is usedIt is a field for adding an encryption key generated in order to carry out data processing with a predetermined algorithm and to read information from said optical disc by optical recordingAn optical disc which is the same format as a recording format of said 1st fieldand has said 1st field and the 2nd field that continues or adjoins.

[Claim 2]A step which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media from said recording mediumAn encryption key generation method which has a step which generates an encryption key for carrying out data processing with a predetermined algorithmand reading information from said recording medium using a step which reads arbitrary passwords which a user of said recording medium sets upand information peculiar to said recording medium and said password.

[Claim 3]A step which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media from said recording mediumA step which reads arbitrary passwords which a user of said recording medium sets upA step which reads information which specifies at least one of two or more of the information currently recorded on said recording medium which said user sets upAn encryption key generation method which has a step which generates an encryption key for carrying out data processing with a predetermined algorithmand reading information from said recording medium using information peculiar to said recording mediumsaid passwordand information that specifies at least one of said two or more of the information.

[Claim 4]A step which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media from said recording mediumA step which reads arbitrary passwords which a user of said recording medium sets upA step which generates an encryption key for carrying out data processing with a predetermined algorithmand reading information on said recording medium using information peculiar to said recording mediumand said passwordAn encryption key record method which has a step which adds said encryption key to a field where information peculiar to said recording medium is recordedand a field which continues or adjoins.

[Claim 5]A step which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media from said recording mediumA step which reads arbitrary passwords which a user of said recording medium sets upA step which reads information which specifies at least one of two or more of the information currently recorded on said recording medium which said user sets upA step which generates an encryption key for carrying out data processing with a predetermined algorithmand reading information on said recording medium using information peculiar to said recording mediumsaid passwordand information that specifies at

least one of said two or more of the informationAn encryption key record method which has a step which adds said encryption key to a field where information peculiar to said recording medium is recordedand a field which continues or adjoins.
[Claim 6]A means which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media from said recording mediumA means to read arbitrary passwords which a user of said recording medium sets upAn encryption key recorder which has a means to transmit information peculiar to said recording mediumand said password to a predetermined encryption key generating devicea means to receive an encryption key from said encryption key generating deviceand a means to add said encryption key to a field where information peculiar to said recording medium is recordedand a field which continues or adjoins.
[Claim 7]A means which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media from said recording mediumA means to read arbitrary passwords which a user of said recording medium sets upA means to read information which specifies at least one of two or more of the information currently recorded on said recording medium which said user sets upInformation peculiar to said recording mediumsaid passwordand a means to transmit information which specifies at least one of said two or more of the information to a predetermined encryption key generating deviceAn encryption key recorder which has a means to receive an encryption key from said encryption key generating deviceand a means to add said encryption key to a field where information peculiar to said recording medium is recordedand a field which continues or adjoins.
[Claim 8]In information and information for discriminating from other recording media reproducing information with playback equipment from a recording medium recorded beforehandA step which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA step which reads an encryption key recorded on a field where information peculiar to said recording medium was recordedand a field which continues or adjoinsA step which generates a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumand said encryption keyAn information reproduction mode which has a step which permits reproduction of a part or all of information currently recorded on said recording medium based on said password.
[Claim 9]In information and information for discriminating from other recording media reproducing information with playback equipment from a recording medium recorded beforehandA step which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA step which reads an encryption key recorded on a field where information peculiar to said recording medium was recordedand a field which continues or adjoinsA step which

generates a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumsaid encryption keyand information that specifies at least one of two or more of the information currently recorded on said recording mediumAn information reproduction mode which has a step which permits reproduction of a part or all of information currently recorded on said recording medium based on said password.

[Claim 10]In information and information for discriminating from other recording media reproducing information with playback equipment from a recording medium recorded beforehandA step which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA step which reads an encryption key recorded on a field where information peculiar to said recording medium was recordedand a field which continues or adjoinsA step which generates information which specifies at least one of two or more of the information currently recorded on said recording medium based on a step which reads a password which a user inputsand information peculiar to said recording mediumsaid encryption key and said passwordAn information reproduction mode which has a step which permits reproduction of a part or all of information currently recorded on said recording medium based on information which specifies at least one of said two or more of the information.

[Claim 11]A user is in charge of reproducing information with playback equipment from a recording medium with which information and information peculiar to said recording medium for discriminating from other recording media were recorded beforehandInformation peculiar to said recording medium which is the information reproduction permission method of judging whether reproduction of information by said user being permittedand was read from said recording medium in the donor side of said recording mediumA step which receives a password which said user inputted from said playback equipment sideIt adds to information peculiar to said recording mediumsaid passwordor theseA step which generates an encryption key for playing a part or all of information that was recorded on said recording medium based on information which specifies at least one of two or more of the information currently recorded on said optical discAn information reproduction permission method of having a step which transmits said encryption key to said playback equipment side in order to permit reproduction of a part or all of information currently recorded on said recording medium.

[Claim 12]Information and information for discriminating from other recording media are playback equipment which reproduces information from a recording medium recorded beforehandA means which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA means which reads an encryption key recorded on a field where information peculiar to said recording medium was recordedand a field which continues or adjoinsAn information reproducing device which has a means to generate a

password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumand said encryption keyand a means to permit reproduction of a part or all of information currently recorded on said recording medium based on said password.
[Claim 13]Information and information for discriminating from other recording media are playback equipment which reproduces information from a recording medium recorded beforehandA means which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA means which reads an encryption key recorded on a field where information peculiar to said recording medium was recordedand a field which continues or adjoinsA means to generate a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumsaid encryption keyand information that specifies at least one of two or more of the information currently recorded on said recording mediumAn information reproducing device which has a means to permit reproduction of a part or all of information currently recorded on said recording medium based on said password.
[Claim 14]A field where optical recording of the information peculiar to said optical disc that an optical disc in which information was recorded is discriminated from other optical discs was carried outIt adds to information peculiar to said optical discarbitrary passwordsor theseAn optical disc which has a field which carries out magnetic recording of the encryption key generated in order to carry out data processing with a predetermined algorithm and to read information from said optical disc using information which specifies at least one of two or more of the information currently recorded on said optical disc.
[Claim 15]A step which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media from said recording mediumA step which reads arbitrary passwords which a user of said recording medium sets upAn encryption key record method which has a step which generates an encryption key for carrying out data processing with a predetermined algorithmand reading information on said recording medium using information peculiar to said recording mediumand said passwordand a step which records said encryption key on a magnetic recording area in which it was provided by said recording medium.
[Claim 16]A step which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media from said recording mediumA step which reads arbitrary passwords which a user of said recording medium sets upA step which reads information which specifies at least one of two or more of the information currently recorded on said recording medium which said user sets upA step which generates an encryption key for carrying out data processing with a predetermined algorithmand reading information on said recording medium using information peculiar to said recording mediumsaid passwordand information that specifies at

least one of said two or more of the informationAn encryption key record method which has a step which records said encryption key on a magnetic recording area in which it was provided by said recording medium.
[Claim 17]A means which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media from said recording mediumA means to read arbitrary passwords which a user of said recording medium sets upAn encryption key recorder which has a means to transmit information peculiar to said recording mediumand said password to a predetermined encryption key generating devicea means to receive an encryption key from said encryption key generating deviceand a means to record said encryption key on a magnetic recording area in which it was provided by said recording medium.
[Claim 18]A means which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media from said recording mediumA means to read arbitrary passwords which a user of said recording medium sets upA means to read information which specifies at least one of two or more of the information currently recorded on said recording medium which said user sets upInformation peculiar to said recording mediumsaid passwordand a means to transmit information which specifies at least one of said two or more of the information to a predetermined encryption key generating deviceAn encryption key recorder which has a means to receive an encryption key from said encryption key generating deviceand a means to record said encryption key on a magnetic recording area in which it was provided by said recording medium.
[Claim 19]In information and information for discriminating from other recording media reproducing information with playback equipment from a recording medium recorded beforehandA step which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA step which reads an encryption key recorded on a magnetic recording area established in said recording mediumA step which generates a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumand said encryption keyAn information reproduction mode which has a step which permits reproduction of a part or all of information currently recorded on said recording medium based on said password.
[Claim 20]In information and information for discriminating from other recording media reproducing information with playback equipment from a recording medium recorded beforehandA step which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA step which reads an encryption key recorded on a magnetic recording area established in said recording mediumA step which generates a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumsaid encryption keyand information that specifies

at least one of two or more of the information currently recorded on said recording mediumAn information reproduction mode which has a step which permits reproduction of a part or all of information currently recorded on said recording medium based on said password.

[Claim 21]In information and information for discriminating from other recording media reproducing information with playback equipment from a recording medium recorded beforehandA step which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA step which reads an encryption key recorded on a magnetic recording area established in said recording mediumA step which generates information which specifies at least one of two or more of the information currently recorded on said recording medium based on a step which reads a password which a user inputsand information peculiar to said recording mediumsaid encryption key and said passwordAn information reproduction mode which has a step which permits reproduction of a part or all of information currently recorded on said recording medium based on information which specifies at least one of said two or more of the information.

[Claim 22]Information and information for discriminating from other recording media are playback equipment which reproduces information from a recording medium recorded beforehandA means which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA means which reads an encryption key recorded on a magnetic recording area established in said recording mediumAn information reproducing device which has a means to generate a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumand said encryption keyand a means to permit reproduction of a part or all of information currently recorded on said recording medium based on said password.

[Claim 23]Information and information for discriminating from other recording media are playback equipment which reproduces information from a recording medium recorded beforehandA means which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA means which reads an encryption key recorded on a magnetic recording area established in said recording mediumA means to generate a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumsaid encryption keyand information that specifies at least one of two or more of the information currently recorded on said recording mediumAn information reproducing device which has a means to permit reproduction of a part or all of information currently recorded on said recording medium based on said password.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention about management of the reproducing permission at the time of playing the information currently recorded on optical discssuch as DVD (digital videodisc: digital versatile disc)It is related with the optical disc which can prevent especially an unauthorized use and an illegal copy (what is called a pirate edition)an encryption key generation methodan encryption key record methodan encryption key recorderan information reproduction modethe information reproduction permission methodand an information reproducing device.
[0002]
[Description of the Prior Art]Generallysince all the information currently recorded on the disk is disclosed by the disk owner as for disk package mediasuch as CDwhen a disk owner obtains a diskhe can use all the information currently recorded on the disk. Thereforeas shown in (b) of drawing 7the remuneration of a disk is set up to all the information currently recorded on the diskConsumers can use all the information which becomes a disk owner and is recorded on the disk as a result by paying the remuneration and purchasing a disk.
[0003]The "superdistribution system" is known as other circulation gestalten. This system is a view which pays a remuneration to not "possession" but "use" of digital informationAs shown in (a) of drawing 7when it applies to DVDthe connector and communication port of an IC card are established in the DVD player which plays the information (soft) currently recordedfor example on the disk. Reproduction limit data is beforehand memorized by the IC cardand this data is reduced for every reproduction of information. It is connected to a soft supplier's computer via a telephone lineand a communication port performs recovery of a DVD reproduction fee and setting out of a reproduction frame.
[0004]By the waysince the disk itself can be manufactured very cheaplymost above-mentioned remunerations are against the quality and quantity of all the information which are recorded on the disk. Howeverin the above systemsthere is a problem that a remuneration must be paid to all the information to play only all the specific information instead of information which are recorded on the disk for the user. Converselya variety of disks into which the contents were changed a little may have to be manufactured beforehand supposing various consumers' demand.
[0005]These are not only inconvenient for consumersbut are a factor which induces a cost hike and the complexity of circulation also for a producer. Although the "superdistribution system" mentioned above solves the above-mentioned problem in respect of the remuneration to informationa large-scale systemsuch as passing a communication network and carrying out the using state and use limitation information of informationis required.
[0006]On the other handafter manufacturing an optical disca part of information storage side of an optical disc is irradiated with a powerful laser beam

etc.Permanent deformation of the reflection film on the substrate and substrate of an optical disc is carried outand the method of recording the information on low density farther than the original storage density of an optical disc is indicated by United States patent 5thNo. 400319etc.for example. since the information which changes for every one disk with such art can be written incan set up the encryption key for every disk and the illicit copy of a disk and an encryption key use about -- ******** -- an unjust act becomes impossible.
[0007]this invention person already Thenfor exampleID peculiar to a recording mediumID of information to reproduceSet up ID of playback equipment beforehand and the technique of generating an encryption key combining at least two of these three ID is developedPatent application is carried out (filing date: December 3 [Reference number:04000675; / Applicant:Victor Company of JapanLtd.]Heisei 8; the name:encryption key generation methodan optical disk playback methodan optical disk reproducing deviceand the optical-disk-reproduction permission method of being an invention;). According to the invention (the time of application of this application unpublished) proposed [this]after an optical disc's coming to handonce a user contacts a soft supplier companyhe can obtain the encryption key which permits playback of the information for which it wishes on condition of the payment of the remuneration of information.
[0008]in the invention proposed [above-mentioned / unpublished]by transmitting information peculiar to a recording mediuminformation peculiar to playback equipmentetc. to the soft supplier side by some meanssuch as a telephonepersonal computer communicationsand mailthe soft supplier side generates an encryption key and provides for a user.
Thereforesince what is necessary is just to transmit the number of a credit card to the soft supplier sidefor examplewithout using an IC card etc. like the above-mentioned superdistribution systemit is convenient and more realistic than a superdistribution system.

[0009]
[Problem(s) to be Solved by the Invention]howeversince optical disc ID etc. are processed with a predetermined algorithm and an encryption key is generated when generating an encryption key using information peculiar to a recording medium according to the invention proposed [above-mentioned / unpublished]if recording media differit will become what differed also in the encryption key. That issince the encryption key for every recording medium is generated when using two or more recording mediait must hold to whether a user memorizes all of these different encryption key and its correspondence recording mediumand memory storageand which encryption key must manage of which recording medium it is a thing. If the number of recording media increasesthis management will be considerable trouble and will serve as a burden for a user.
[0010]thereforethis invention in view of the above-mentioned conventional problem and the problem in the invention proposed [above-mentioned / unpublished]The remuneration and the disk itself of information to a user can be

made cheapand an illegal copy can be prevented by extensionAnd it aims at providing the unnecessary optical discthe encryption key generation methodthe optical disk playback methodoptical disk reproducing deviceand the optical-disk-reproduction permission method of management of the complicated encryption key by a user.

[0011]

[Means for Solving the Problem]This invention reads information peculiar to a recording medium that a recording medium with which information was recorded is discriminated from other recording media to achieve the above objects from a recording mediumRead arbitrary passwords which a user of a recording medium sets upand information and a password peculiar to a recording medium are usedWhen data processing is carried out with a predetermined algorithman encryption key for reading information from a recording medium is generated and a user wants to read informationHe is trying to permit reproduction of a part or all of information currently recorded on a recording medium based on a password inputted at this timeand an encryption key generated previously. Data processing is carried out with a predetermined algorithm also using information which specifies at least one of two or more of the information currently recorded on a recording mediumand it may be made to generate [according to other modes of this invention] an encryption key for reading information from a recording medium in addition to information and a password peculiar to a recording medium. It is a desirable mode of this invention to record an encryption key generated [above-mentioned] on a predetermined record section of a recording medium. It is a desirable mode of this invention to use a field which continues or adjoins a field to which information peculiar to a recording medium is recorded as this predetermined record section. It is a desirable mode of this invention to use a magnetic recording area established in a recording medium as this predetermined record section.

[0012]Namelythe 1st field where optical recording of the information peculiar to said optical disc that an optical disc in which information was recorded is discriminated from other optical discs according to this invention was carried outIt adds to information peculiar to said optical discarbitrary passwordsor theseInformation which specifies at least one of two or more of the information currently recorded on said optical disc is usedIt is a field for adding an encryption key generated in order to carry out data processing with a predetermined algorithm and to read information from said optical disc by optical recordingIt is the same format as a recording format of said 1st fieldand an optical disc which has said 1st field and the 2nd field that continues or adjoins is provided.

[0013]A step which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media according to this invention from said recording mediumUsing a step which reads arbitrary passwords which a user of said recording medium sets upand information peculiar to said recording medium and said passworddata processing is carried out with a predetermined algorithmand an encryption key

generation method which has a step which generates an encryption key for reading information from said recording medium is provided.
[0014]A step which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media according to this invention from said recording mediumA step which reads arbitrary passwords which a user of said recording medium sets upA step which reads information which specifies at least one of two or more of the information currently recorded on said recording medium which said user sets upUsing information peculiar to said recording mediumsaid passwordand information that specifies at least one of said two or more of the informationdata processing is carried out with a predetermined algorithmand an encryption key generation method which has a step which generates an encryption key for reading information from said recording medium is provided.
[0015]A step which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media according to this invention from said recording mediumA step which reads arbitrary passwords which a user of said recording medium sets upA step which generates an encryption key for carrying out data processing with a predetermined algorithmand reading information on said recording medium using information peculiar to said recording mediumand said passwordAn encryption key record method which has a step which adds said encryption key to a field where information peculiar to said recording medium is recordedand a field which continues or adjoins is provided.
[0016]A step which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media according to this invention from said recording mediumA step which reads arbitrary passwords which a user of said recording medium sets upA step which reads information which specifies at least one of two or more of the information currently recorded on said recording medium which said user sets upA step which generates an encryption key for carrying out data processing with a predetermined algorithmand reading information on said recording medium using information peculiar to said recording mediumsaid passwordand information that specifies at least one of said two or more of the informationAn encryption key record method which has a step which adds said encryption key to a field where information peculiar to said recording medium is recordedand a field which continues or adjoins is provided.
[0017]A means which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media according to this invention from said recording mediumA means to read arbitrary passwords which a user of said recording medium sets upA means to transmit information peculiar to said recording mediumand said password to a predetermined encryption key generating deviceAn encryption key recorder which has a means to receive an encryption key from said encryption key generating deviceand a means to add said encryption key to a field where information peculiar

to said recording medium is recordedand a field which continues or adjoins is provided.
[0018]A means which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media according to this invention from said recording mediumA means to read arbitrary passwords which a user of said recording medium sets upA means to read information which specifies at least one of two or more of the information currently recorded on said recording medium which said user sets upInformation peculiar to said recording mediumsaid passwordand a means to transmit information which specifies at least one of said two or more of the information to a predetermined encryption key generating deviceAn encryption key recorder which has a means to receive an encryption key from said encryption key generating deviceand a means to add said encryption key to a field where information peculiar to said recording medium is recordedand a field which continues or adjoins is provided.
[0019]Are in charge of information and information for discriminating from other recording media reproducing information with playback equipment from a recording medium recorded beforehand according to this inventionA step which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA step which reads an encryption key recorded on a field where information peculiar to said recording medium was recordedand a field which continues or adjoinsA step which generates a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumand said encryption keyAn information reproduction mode which has a step which permits reproduction of a part or all of information currently recorded on said recording medium based on said password is provided.
[0020]Are in charge of information and information for discriminating from other recording media reproducing information with playback equipment from a recording medium recorded beforehand according to this inventionA step which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA step which reads an encryption key recorded on a field where information peculiar to said recording medium was recordedand a field which continues or adjoinsA step which generates a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumsaid encryption keyand information that specifies at least one of two or more of the information currently recorded on said recording mediumAn information reproduction mode which has a step which permits reproduction of a part or all of information currently recorded on said recording medium based on said password is provided.
[0021]Are in charge of information and information for discriminating from other recording media reproducing information with playback equipment from a recording

medium recorded beforehand according to this inventionA step which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA step which reads an encryption key recorded on a field where information peculiar to said recording medium was recordedand a field which continues or adjoinsA step which generates information which specifies at least one of two or more of the information currently recorded on said recording medium based on a step which reads a password which a user inputsand information peculiar to said recording mediumsaid encryption key and said passwordAn information reproduction mode which has a step which permits reproduction of a part or all of information currently recorded on said recording medium based on information which specifies at least one of said two or more of the information is provided.

[0022]According to this inventiona user is in charge of reproducing information with playback equipment from a recording medium with which information and information peculiar to said recording medium for discriminating from other recording media were recorded beforehandInformation peculiar to said recording medium which is the information reproduction permission method of judging whether reproduction of information by said user being permittedand was read from said recording medium in the donor side of said recording mediumA step which receives a password which said user inputted from said playback equipment sideIt adds to information peculiar to said recording mediumsaid passwordor theseA step which generates an encryption key for playing a part or all of information that was recorded on said recording medium based on information which specifies at least one of two or more of the information currently recorded on said optical discAn information reproduction permission method of having a step which transmits said encryption key to said playback equipment side in order to permit reproduction of a part or all of information currently recorded on said recording medium is provided.

[0023]According to this inventioninformation and information for discriminating from other recording media are playback equipment which reproduces information from a recording medium recorded beforehandA means which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA means which reads an encryption key recorded on a field where information peculiar to said recording medium was recordedand a field which continues or adjoinsA means to generate a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumand said encryption keyAn information reproducing device which has a means to permit reproduction of a part or all of information currently recorded on said recording medium based on said password is provided.

[0024]According to this inventioninformation and information for discriminating from other recording media are playback equipment which reproduces information

from a recording medium recorded beforehandA means which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA means which reads an encryption key recorded on a field where information peculiar to said recording medium was recordedand a field which continues or adjoinsA means to generate a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumsaid encryption keyand information that specifies at least one of two or more of the information currently recorded on said recording mediumAn information reproducing device which has a means to permit reproduction of a part or all of information currently recorded on said recording medium based on said password is provided.

[0025]A field where optical recording of the information peculiar to said optical disc that an optical disc in which information was recorded is discriminated from other optical discs according to this invention was carried outIt adds to information peculiar to said optical discarbitrary passwordsor theseUsing information which specifies at least one of two or more of the information currently recorded on said optical discdata processing is carried out with a predetermined algorithmand an optical disc which has a field which carries out magnetic recording of the encryption key generated in order to read information from said optical disc is provided.

[0026]A step which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media according to this invention from said recording mediumA step which reads arbitrary passwords which a user of said recording medium sets upA step which generates an encryption key for carrying out data processing with a predetermined algorithmand reading information on said recording medium using information peculiar to said recording mediumand said passwordAn encryption key record method which has a step which records said encryption key on a magnetic recording area in which it was provided by said recording medium is provided.

[0027]A step which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media according to this invention from said recording mediumA step which reads arbitrary passwords which a user of said recording medium sets upA step which reads information which specifies at least one of two or more of the information currently recorded on said recording medium which said user sets upA step which generates an encryption key for carrying out data processing with a predetermined algorithmand reading information on said recording medium using information peculiar to said recording mediumsaid passwordand information that specifies at least one of said two or more of the informationAn encryption key record method which has a step which records said encryption key on a magnetic recording area in which it was provided by said recording medium is provided.

[0028]A means which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other

recording media according to this invention from said recording mediumA means to read arbitrary passwords which a user of said recording medium sets upAn encryption key recorder which has a means to transmit information peculiar to said recording medium and said password to a predetermined encryption key generating devicea means to receive an encryption key from said encryption key generating deviceand a means to record said encryption key on a magnetic recording area in which it was provided by said recording medium is provided.
[0029]A means which reads information peculiar to said recording medium that a recording medium with which information was recorded is discriminated from other recording media according to this invention from said recording mediumA means to read arbitrary passwords which a user of said recording medium sets upA means to read information which specifies at least one of two or more of the information currently recorded on said recording medium which said user sets upInformation peculiar to said recording mediumsaid passwordand a means to transmit information which specifies at least one of said two or more of the information to a predetermined encryption key generating deviceAn encryption key recorder which has a means to receive an encryption key from said encryption key generating deviceand a means to record said encryption key on a magnetic recording area in which it was provided by said recording medium is provided.
[0030]Are in charge of information and information for discriminating from other recording media reproducing information with playback equipment from a recording medium recorded beforehand according to this inventionA step which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA step which reads an encryption key recorded on a magnetic recording area established in said recording mediumA step which generates a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumand said encryption keyAn information reproduction mode which has a step which permits reproduction of a part or all of information currently recorded on said recording medium based on said password is provided.
[0031]Are in charge of information and information for discriminating from other recording media reproducing information with playback equipment from a recording medium recorded beforehand according to this inventionA step which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA step which reads an encryption key recorded on a magnetic recording area established in said recording mediumA step which generates a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumsaid encryption keyand information that specifies at least one of two or more of the information currently recorded on said recording mediumAn information reproduction mode which has a step which permits reproduction of a part or all of information currently recorded on said recording medium based on

said password is provided.
[0032]Are in charge of information and information for discriminating from other recording media reproducing information with playback equipment from a recording medium recorded beforehand according to this inventionA step which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA step which reads an encryption key recorded on a magnetic recording area established in said recording mediumA step which generates information which specifies at least one of two or more of the information currently recorded on said recording medium based on a step which reads a password which a user inputsand information peculiar to said recording mediumsaid encryption key and said passwordAn information reproduction mode which has a step which permits reproduction of a part or all of information currently recorded on said recording medium based on information which specifies at least one of said two or more of the information is provided.
[0033]According to this inventioninformation and information for discriminating from other recording media are playback equipment which reproduces information from a recording medium recorded beforehandA means which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA means which reads an encryption key recorded on a magnetic recording area established in said recording mediumA means to generate a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumand said encryption keyAn information reproducing device which has a means to permit reproduction of a part or all of information currently recorded on said recording medium based on said password is provided.
[0034]According to this inventioninformation and information for discriminating from other recording media are playback equipment which reproduces information from a recording medium recorded beforehandA means which reads information peculiar to said recording medium that a recording medium with which said information was recorded is discriminated from other recording media from said recording mediumA means which reads an encryption key recorded on a magnetic recording area established in said recording mediumA means to generate a password for reproducing a part or all of information that was recorded on said recording medium based on information peculiar to said recording mediumsaid encryption keyand information that specifies at least one of two or more of the information currently recorded on said recording mediumAn information reproducing device which has a means to permit reproduction of a part or all of information currently recorded on said recording medium based on said password is provided.
[0035]
[Embodiment of the Invention]Hereafteran embodiment of the invention is described with reference to drawings. The explanatory view showing one

embodiment of an encryption key generation methodan optical disk playback methodan optical disk reproducing deviceand the optical-disk-reproduction permission method which drawing 1 requires for this inventionDrawing 2 is a flow chart for explaining the processing in the optical disk reproducing device of drawing 1and drawing 3 is a flow chart for explaining the processing in the software house of drawing 1.

[0036]Drawing 1 plays as an example the optical disc 1 in which game software was recorded with the disk reproduction device 2The system by which the software house 3 which is a donor of software (below soft) collects the remuneration of playback from the user of the disk reproduction device 2 is shownand a user is provided with the disk 1 no charge or very cheaply as an appendix of a magazine etc. in this system (graphic display **). The peculiar information (henceforthdisk ID) which discriminates 50 game software and disks 1 from other disks is recorded on the information area of the disk 1. Peculiar information (the followingtitle key) is set up in the form which includes each game software of every or all the game softwareand this title key and soft consecutive numbers correspond by 1 to 1 at this embodiment. The file name of a title key and softwareetc. may be made to correspond instead. The disk reproduction device 2 which is a software house [which is a disk donor] 3and user side can communicate mutually via a communication line etc.and assumes that it has CPU (central processing unit) and the interface of a graphic display abbreviationrespectively so that it may mention later.

[0037]Even if an encryption key is not inputtedthe address information of the area (for examplethe 1st scene for every software) which permits playbackand the address information of the area (soft main part) which permits playback on condition of the input of an encryption key are recorded on the sector header of the disk 1. And the disk reproduction device 2 has the 1st refreshable scene of software for every softwarewhen playing the disk 1but it is constituted so that it cannot playunless an encryption key is inputted after that [the / soft].

[0038]As a record method of disk IDas shownfor example in a U.S. Pat. No. 5400319 itemAfter recording the information on low density on the surface of the disk 1 farther than storage densityBy irradiating with the powerful laser beam modulated according to the binary data "1" which shows disk IDand "0"and carrying out permanent deformation of the reflection film of the disk 1 in the position of data "1"as shown in "those with reflective =1"and "reflective nothing =0"it is recordable as a bar code. According to this embodimentthe BCA number used in DVD as an example of disk ID is recordedand this BCA number is read by the disk reproduction device 2for exampleit is displayed by a decimal digit.

[0039]Ranging over two or more tracks of the most-inner-circumference portion of the optical recording portion of an optical discBCA(s) are the field which formed the bar code in the optical beam with a powerful YAG laser beam etc.and a field which can add a bar codeand also call it burst cutting area. A BCA number means information peculiar to one-sheet the disk of one sheet in the information recorded on BCA as a bar code. The portion by other recording methodssuch as a

magnetic recording areais provided not only in BCA but in a diskand it may be made to read this to it with a head for exclusive use.
[0040]The ten key for a user to input a password into the disk reproduction device 2 is formed. It is used as a code for generating the title key encryption key as information which specifies at least one of this passwordthe BCA number mentioned aboveand two or more of the information currently recorded on the optical disc 1.
[0041]In the disk reproduction device 2if the disk 1 is seteven if there is no encryption keyonly the area which permits playback will be played and displayed. Although the user can know a desired soft outline or beginning portion to reproduce by thisthe soft encryption key is unknown for a user. Herethe title key of a desired soft number "01" is set to "08001" as an example.
[0042]The disk reproduction device 2 and a user via a modema PB signal and a telephone lineor an ISDN circuit as opposed to the software house 3 Firstthe BCA number (for example00123) of the - disk 1- The password (for example01010) which a user sets up arbitrarilythe credit card number for - remuneration paymentand the soft number "01" of - request
********** (graphic display **). in this casethe encryption key which permits reproduction -- for example [0043]
[Equation 1]
Encryption key ="title key"-"BCA number"- "password"
=08001-00123-01010 =06868[0044]It carries out. Subsequentlythe software houses 3 are the conditions which pay the remuneration which plays the soft number "01" of the disk 1and send this encryption key to the disk reproduction device 2for example using a modem etc. (graphic display **).
[0045]It is what showed drawing 2 - procedure [in / in six / the disk reproduction device 2 and the software house 3]and signs that an encryption key is generated via communication with the software house 3 of drawing 1and a password is generated using it are shown. Drawing 2 shows first the procedure which transmits each predetermined information to the software house 3 in the disk reproduction device 2. Firstdisk ID is read at Step S1and the input of a password is required of a user at Step S2. A user decides arbitrary passwords and inputs this using the ten key of a graphic display abbreviation of the disk reproduction device 3. If the input of a password is checked at Step S3the input of a soft number to reproduce by step S4 will be requiredand the input will be checked at Step S5. Subsequentlythe input of a credit card number is required at Step S6and the input is checked at Step S7. If each of these information is inputtedeach information will be transmitted to the software house 3 at Step S8the completion of transmitting will be checkedand transmitting processing will be ended.
[0046]Drawing 3 is a flow chart which shows procedure by the side of the software house 3. In the software house 3a check of having received a useri.e.information from the disk reproduction device 2at Step S11 will transmit to a user an encryption key which generated an encryption key and was subsequently generated by the above-mentioned technique at Step S12 at Step S13. If the

completion of transmitting is checked at Step S14with a credit card number of a user received at Step S15predetermined accounting will be performed and processing by the side of the software house 3 will be ended.
[0047]Drawing 4 shows a procedure which writes an encryption key transmitted from the software house 3 in the optical disc 1 in the disk reproduction device 2. That isif reception of an encryption key is checked at Step S18an encryption key received to a predetermined region of a disk at Step S19 will be written inan end of writing will be checked at Step S20and processing will be ended. Thereforethe disk reproduction device will operate also as an encryption key postscript device. A postscript region of BCA can be used as a predetermined region of a disk. Disk ID is a part of BCA currently recorded as a BCA numberand a postscript region of this BCA is a field which continues or adjoins a field to which a BCA number is recorded. There is a portion which there is a bar code postscript feasible region of a consecutive part of a circumferencial direction of a record section of disk ID in BCAand adjoins a radial direction of a disk similarly as an adjoining field as a continuous field and which can be bar code added.
[0048]Nextdrawing 5 explains a procedure for playing desired information from the optical disc 1. Drawing 5 is a flow chart which shows procedure of a reproducing permission in the disk reproduction device 2. Nowan encryption key generated in a software house shall be recorded on the optical disc 1 by processing of drawing 4 explained previously. Disk ID is read at Step S21andsubsequently an encryption key is read at Step S22. Each of these information is recorded on BCAand is read as a bar code. If existence of an encryption key is checked at Step S23a title key will be detected at Step S24. Detection of a title key is finding out a number corresponding to a soft number which a user inputs to reproduce by 1 to 1for examplethe title key 08001 corresponding to the soft number 001 is detected.
[0049]In Step S25as shown in a following formula using Step S21disk ID read by S22and a title key detected at an encryption key and Step S24a password is computed.
[0050]
[Equation 2]
Password ="title key"-"BCA number"- "encryption key"
=08001-00123-06868 =01010[0051]In this waythe computed password is called calculation password. Nextthe input of a password is required of a user at Step S26. This password is called input password. If whether the input password was inputted judges and it is inputted at Step S27it will be judged whether an input password is in agreement with a calculation password at Step S28. If in agreementin order to permit playback of an applicable title at Step S29playback of the soft number "01" of the disk 1 corresponding to a title key "08001" is permittedLet reproduction be disapproval so that you cannot perform soft reproduction at Step S30when not in agreementand when an encryption key is not detected at Step S23.
[0052]Although a password is computed and it judges whether it is in agreement with a password which a user inputted in the above-mentioned exampleit may be

made to compute a title key not only using this but using an inputted password. Drawing 6 is a flow chart which shows a procedure in a case of judging whether a title key is computed and soft reproduction is permitted. The same step number shows the same step as drawing 5and it omits the explanation. In a flow chart of drawing 6if an input of a password will be required of a user at Step S26 if existence of an encryption key is checked at Step S23and the input is checked at Step S27as shown in a following formulaa title key will be computed at Step S31.
[0053]
[Equation 3]
Title key ="BCA number"+ "encryption key" + "password"
=00123+06868+01010 =08001[0054]Subsequentlyit is judged whether the title corresponding to the title key computed at Step S32 exists in the optical disc 1. When it existsreproduction of an applicable title is permitted at Step S29. On the other handwhen an applicable title does not existand when an encryption key is not detected at Step S23let reproduction be disapproval at Step S30.
[0055]Namelyeven if the user of the disk reproduction device 2 holds the disk 1about the information which does not need to pay the software house 3 a remunerationit is freely renewablebut. It is unreproducibleunless it pays the software house 3 a remuneration about subsequent information and learning of the encryption key is carried out from the software house 3.
[0056]In the above-mentioned examplealthough disk ID set to 00123the case where information is played from another disk now is examined. Disk ID of this another disk is set to 00150. As drawing 3 explained previouslyan encryption key is generated in the software house 3but an encryption key will be set to 06841if a password sets to 1010 by disk ID setting to 00150 and a title key sets to 8001. This new encryption key is recorded on this disk by processing of drawing 4. A password or a title key is generated by this encryption key. Thereforewhen playing information from this diskdesired software can be played by inputting the same password 01010 as the time of disk ID explained previously being a disk of 00123.
[0057]Although the above-mentioned example explained a generated encryption key as what is recorded on a field which continues or adjoins a record section of a postscript portion of BCAi.e.disk IDAn encryption key is also recordable on a magnetic recording area further established in what is called a label segment of inner circumference from an optical recording area of a disk by magnetic recording.
[0058]A generation method of the above-mentioned encryption key is for simplifying explanationand since actually raises securityit is generated based on complicated code generation logic (algorithm). A digit number of disk ID and a password is also an examplefor examplenot a number but a character and a sign of the alphabet may be used for a passwordor a digit number may also be changed into it as a combination of a number and a character. Many digit numbers of a password can be said to be strong to an unauthorized use so that there arebut since memory and an input will become troublesome if there are not much many digit numberswithin the limits of 1 thru/or 30 bytes is desired.
[0059]Although the above-mentioned embodiment explains as information which

specifies one of two or more of the information recorded on a disk in a title keyit can also treat as reproduction permission information over information on an entire disk. It can also be dealt with as information which specifies combination of two or more information recorded on a disk in a title key. For examplesince 32 kinds of information can be specified corresponding to each bit if 4 bytes = 32 bits are assigned as a title keya title key can be treated as reproduction permission information over two or more information.

[0060]Disk ID may not necessarily be the BCA number itselfand it may be encoded within playback equipment so that information on a BCA number may be included correctly. In this casealthough playback equipment also needs to have a function of decodingit is a technique effective in improvement in privacy of an encryption key. Although a disk reproduction device explained in the above-mentioned example as what operates also as an encryption key postscript deviceA function concerning a disk reproduction device is not givenbut an encryption key postscript device is formed separatelyand an encryption key received to the encryption key postscript device is inputtedand a postscript may be added to disk ID areas as a bar codeand it may be made to add a postscript to a magnetic recording area by magnetic recording.

[0061]An encryption key replied from soft supply origin may be encoded by form which may not necessarily be the encryption key itself and is not [user sudden]. In that casethis data is decoded at the time of encryption key record or encryption key read-out of disk reproductionand a title key is generated. Encryption key information added to a disk ID record sectionA password can be changedif that is anew connected to a soft supplier when a password which a user set up becomes what has bad convenience temporarilysince a postscript can be added as long as a non-record section remains in a disk ID record sectionand rewriting is possible in false. In a disk provided with a magnetic recording areasince encryption key information recorded on a magnetic recording area is rewritablewhen a password which a user set up becomes what has bad convenience temporarilyif that is anew connected to a soft suppliera password can be changed. What is necessary is just to rewrite to a new encryption key in a form which adds a new encryption key or includes old encryption key informationwhen similarly information included in a disk wants to add those with two or moreand information to use later. Under the present circumstancessince the same password as before can be usedit is convenient.

[0062]A different password to two or more information can also be set upand reproduction restrictions can also be applied in combination of arbitrary titles. Information which specifies at least one of two or more information recorded on a recording medium is synonymous with information to which at least one reproduction is permitted among two or more information recorded on a recording mediumand is the reproduction limit information itself. Thereforeinformation used as a title key in an example is good also as reproduction limit informationand when the number of titles is one (information is one)it is equivalent to reproduction permission information of a recording medium.

[0063]Thereforesince what is necessary is just to pay a remuneration to the information according to such a method to play only all the specific information instead of information which are recorded on the disk 1 for a userunjust playback can be prevented while a remuneration becomes cheap. Since the disk 1 with which much information was recorded by this can be mass-producedthe disk 1 can be made cheapand a pirate edition will not be overruneitherif the disk 1 is cheap.
[0064]
[Effect of the Invention]Since an encryption key is automatically generated using the password which the user set up arbitrarily according to this invention as explained abovemanagement of the complicated encryption key by a user is unnecessaryand selective reproduction permission of information can be realized using a password common to two or more disks. Thereforewhile a user's convenience is plannedthe remuneration and the disk itself of information can be made cheapand an illegal copy can be prevented.
[0065]Since a disk can be distributed cheaplythey will not have useless expenses since consumers should pay a remuneration only to the information part which ones need and a disk will circulate very cheaply in order to charge to the information itself if the effect of this invention is arrangedSince the circulation place of a disk is certainly known when a pirate edition is not materialized but there is a request of encryption key distribution from a userSince user management can be done certainlyand the purchase of information can be performed after grasp of an inaccurate copy disk is also easyand a cheap disk comes to hand for the time being and checking the contents in the non-code portion of each softwareSince a user can set up a password arbitrarily in addition to the fundamental advantage that circulation becomes activeSince the encryption key which can also set up the same number to all the possession disksdoes not need to keep a password in mind for every diskand is transmitted by the soft supplier is effective only to the diskSince what is necessary is just to contact a soft supplier once again to change a password once it is not abused to other disks and registers to a certain disk and a certain soft supplierThe addition of information to use to the disk with which it can change and two or more information is included is possible for a password alwaysThe same password can be used also in that case and it is effective also in changingof course being also possible and being able to set up a different password to further two or more information.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is an explanatory view showing one embodiment of an encryption key generation methodan optical disk playback methodan optical disk reproducing deviceand the optical-disk-reproduction permission method concerning this invention.

[Drawing 2]It is a flow chart for explaining transmitting processing of the information in the optical disk reproducing device of drawing 1.
[Drawing 3]It is a flow chart for explaining the encryption key generation in a software house and its transmitting processing of drawing 1.
[Drawing 4]It is a flow chart for explaining reception and the writing processing to a disk of the encryption key in the optical disk reproducing device of drawing 1.
[Drawing 5]It is a flow chart for explaining an example of processing of the reproducing permission and prohibition in the optical disk reproducing device of drawing 1.
[Drawing 6]It is a flow chart for explaining other examples of processing of the reproducing permission and prohibition in the optical disk reproducing device of drawing 1.
[Drawing 7]It is a figure showing typically the conventional soft supply form between a software house and a user.
[Description of Notations]
1 Optical disc
2 Optical disk reproducing device
2a Memory
3 Software house

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－208388

(43)公開日　平成10年(1998)８月７日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ
Ｇ１１Ｂ　7/00		Ｇ１１Ｂ　7/00	Ｒ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ

審査請求　未請求　請求項の数23　ＦＤ　（全 15 頁）

(21)出願番号　特願平9－21989

(22)出願日　平成９年(1997)１月21日

(71)出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町３丁目12番地

(72)発明者　望月　聖樹
神奈川県横浜市神奈川区守屋町３丁目12番地　日本ビクター株式会社内

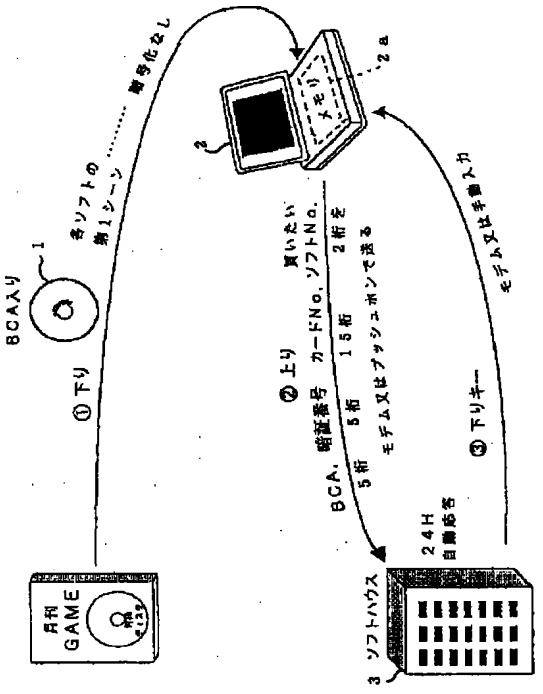
(74)代理人　弁理士　二瓶　正敬

(54)【発明の名称】　光ディスク、暗号鍵生成方法、暗号鍵記録方法、暗号鍵記録装置、情報再生方法、情報再生許可方法、並びに情報再生装置

(57)【要約】

【課題】　利用者に対する情報の対価とディスク自体を安価にし、不正コピーを防止するとともに暗号鍵の管理を容易にする。

【解決手段】　ディスク再生装置２にて情報が記録された記録媒体１を他の記録媒体から識別する記録媒体固有の情報を記録媒体から読み出し、記録媒体のユーザが設定する任意の暗証番号を読み取り、ソフトハウス３にて記録媒体固有の情報と暗証番号とを用いて、所定のアルゴリズムにて演算処理し、記録媒体から情報を読み出すための暗号鍵を生成しておき、ユーザが情報を読み出したいときは、ディスク再生装置２にてこの時点で入力された暗証番号と先に生成された暗号鍵に基づいて記録媒体に記録されている情報の一部又は全部の再生を許可するようにしている。



【特許請求の範囲】
【請求項１】　情報が記録された光ディスクを他の光ディスクから識別する前記光ディスク固有の情報が光記録された第１領域と、
前記光ディスク固有の情報と任意の暗証番号と、又はこれらに加えて、前記光ディスクに記録されている複数の情報の少なくとも１つを特定する情報とを用いて、所定のアルゴリズムにて演算処理し、前記光ディスクから情報を読み出すために生成された暗号鍵を光記録により追記するための領域であって、前記第１領域の記録フォーマットと同一フォーマットであり、かつ前記第１領域と連続又は隣接する第２領域とを、
有する光ディスク。
【請求項２】　情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出すステップと、
前記記録媒体のユーザが設定する任意の暗証番号を読み取るステップと、
前記記録媒体固有の情報と前記暗証番号とを用いて、所定のアルゴリズムにて演算処理し、前記記録媒体から情報を読み出すための暗号鍵を生成するステップとを、
有する暗号鍵生成方法。
【請求項３】　情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出すステップと、
前記記録媒体のユーザが設定する任意の暗証番号を読み取るステップと、
前記ユーザが設定する前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報を読み取るステップと、
前記記録媒体固有の情報と前記暗証番号と前記複数の情報の少なくとも１つを特定する情報とを用いて、所定のアルゴリズムにて演算処理し、前記記録媒体から情報を読み出すための暗号鍵を生成するステップとを、
有する暗号鍵生成方法。
【請求項４】　情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出すステップと、
前記記録媒体のユーザが設定する任意の暗証番号を読み取るステップと、
前記記録媒体固有の情報と前記暗証番号とを用いて、所定のアルゴリズムにて演算処理し、前記記録媒体の情報を読み出すための暗号鍵を生成するステップと、
前記暗号鍵を前記記録媒体固有の情報が記録されている領域と連続又は隣接する領域に追記するステップとを、
有する暗号鍵記録方法。
【請求項５】　情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出すステップと、
前記記録媒体のユーザが設定する任意の暗証番号を読み取るステップと、
前記ユーザが設定する前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報を読み取るステップと、
前記記録媒体固有の情報と前記暗証番号と前記複数の情報の少なくとも１つを特定する情報とを用いて、所定のアルゴリズムにて演算処理し、前記記録媒体の情報を読み出すための暗号鍵を生成するステップと、
前記暗号鍵を前記記録媒体固有の情報が記録されている領域と連続又は隣接する領域に追記するステップとを、
有する暗号鍵記録方法。
【請求項６】　情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出す手段と、
前記記録媒体のユーザが設定する任意の暗証番号を読み取る手段と、
前記記録媒体固有の情報と前記暗証番号とを所定の暗号鍵生成装置に送信する手段と、
前記暗号鍵生成装置から暗号鍵を受信する手段と、
前記暗号鍵を前記記録媒体固有の情報が記録されている領域と連続又は隣接する領域に追記する手段とを、
有する暗号鍵記録装置。
【請求項７】　情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出す手段と、
前記記録媒体のユーザが設定する任意の暗証番号を読み取る手段と、
前記ユーザが設定する前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報を読み取る手段と、
前記記録媒体固有の情報と前記暗証番号と前記複数の情報の少なくとも１つを特定する情報を所定の暗号鍵生成装置に送信する手段と、
前記暗号鍵生成装置から暗号鍵を受信する手段と、
前記暗号鍵を前記記録媒体固有の情報が記録されている領域と連続又は隣接する領域に追記する手段とを、
有する暗号鍵記録装置。
【請求項８】　情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生装置にて再生するにあたり、
前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出すステップと、
前記記録媒体固有の情報の記録された領域と連続又は隣接する領域に記録された暗号鍵を読み出すステップと、
前記記録媒体固有の情報と前記暗号鍵とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成するステップと、
前記暗証番号に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可するステップとを、

有する情報再生方法。
【請求項９】　情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生装置にて再生するにあたり、
前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出すステップと、
前記記録媒体固有の情報の記録された領域と連続又は隣接する領域に記録された暗号鍵を読み出すステップと、
前記記録媒体固有の情報と前記暗号鍵と前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成するステップと、
前記暗証番号に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可するステップとを、
有する情報再生方法。
【請求項１０】　情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生装置にて再生するにあたり、
前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出すステップと、
前記記録媒体固有の情報の記録された領域と連続又は隣接する領域に記録された暗号鍵を読み出すステップと、
ユーザが入力する暗証番号を読み取るステップと、
前記記録媒体固有の情報と前記暗号鍵と前記暗証番号とに基づいて前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報を生成するステップと、
前記複数の情報の少なくとも１つを特定する情報に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可するステップとを、
有する情報再生方法。
【請求項１１】　情報と、他の記録媒体から識別するための前記記録媒体固有の情報とがあらかじめ記録された記録媒体からユーザが情報を再生装置にて再生するにあたり、前記記録媒体の提供者側にて前記ユーザによる情報の再生を許可するか否かを判断する情報再生許可方法であって、
前記記録媒体から読み出された前記記録媒体固有の情報と、前記ユーザが入力した暗証番号を前記再生装置側から受信するステップと、
前記記録媒体固有の情報と、前記暗証番号と、又はこれらに加えて、前記光ディスクに記録されている複数の情報の少なくとも１つを特定する情報とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗号鍵を生成するステップと、
前記記録媒体に記録されている情報の一部又は全部の再生を許可するために前記暗号鍵を前記再生装置側に送信するステップとを、
有する情報再生許可方法。
【請求項１２】　情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生する再生装置であって、
前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出す手段と、
前記記録媒体固有の情報の記録された領域と連続又は隣接する領域に記録された暗号鍵を読み出す手段と、
前記記録媒体固有の情報と前記暗号鍵とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成する手段と、
前記暗証番号に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可する手段とを、
有する情報再生装置。
【請求項１３】　情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生する再生装置であって、
前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出す手段と、
前記記録媒体固有の情報の記録された領域と連続又は隣接する領域に記録された暗号鍵を読み出す手段と、
前記記録媒体固有の情報と前記暗号鍵と前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成する手段と、
前記暗証番号に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可する手段とを、
有する情報再生装置。
【請求項１４】　情報が記録された光ディスクを他の光ディスクから識別する前記光ディスク固有の情報が光記録された領域と、
前記光ディスク固有の情報と任意の暗証番号と、又はこれらに加えて、前記光ディスクに記録されている複数の情報の少なくとも１つを特定する情報とを用いて、所定のアルゴリズムにて演算処理し、前記光ディスクから情報を読み出すために生成された暗号鍵を磁気記録する領域とを、
有する光ディスク。
【請求項１５】　情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出すステップと、
前記記録媒体のユーザが設定する任意の暗証番号を読み取るステップと、
前記記録媒体固有の情報と前記暗証番号とを用いて、所定のアルゴリズムにて演算処理し、前記記録媒体の情報を読み出すための暗号鍵を生成するステップと、
前記暗号鍵を前記記録媒体に設けられた磁気記録領域に記録するステップとを、

有する暗号鍵記録方法。
【請求項１６】　情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出すステップと、
前記記録媒体のユーザが設定する任意の暗証番号を読み取るステップと、
前記ユーザが設定する前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報を読み取るステップと、
前記記録媒体固有の情報と前記暗証番号と前記複数の情報の少なくとも１つを特定する情報とを用いて、所定のアルゴリズムにて演算処理し、前記記録媒体の情報を読み出すための暗号鍵を生成するステップと、
前記暗号鍵を前記記録媒体に設けられた磁気記録領域に記録するステップとを、
有する暗号鍵記録方法。
【請求項１７】　情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出す手段と、
前記記録媒体のユーザが設定する任意の暗証番号を読み取る手段と、
前記記録媒体固有の情報と前記暗証番号とを所定の暗号鍵生成装置に送信する手段と、
前記暗号鍵生成装置から暗号鍵を受信する手段と、
前記暗号鍵を前記記録媒体に設けられた磁気記録領域に記録する手段とを、
有する暗号鍵記録装置。
【請求項１８】　情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出す手段と、
前記記録媒体のユーザが設定する任意の暗証番号を読み取る手段と、
前記ユーザが設定する前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報を読み取る手段と、
前記記録媒体固有の情報と前記暗証番号と前記複数の情報の少なくとも１つを特定する情報を所定の暗号鍵生成装置に送信する手段と、
前記暗号鍵生成装置から暗号鍵を受信する手段と、
前記暗号鍵を前記記録媒体に設けられた磁気記録領域に記録する手段とを、
有する暗号鍵記録装置。
【請求項１９】　情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生装置にて再生するにあたり、
前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出すステップと、
前記記録媒体に設けられた磁気記録領域に記録された暗号鍵を読み出すステップと、
前記記録媒体固有の情報と前記暗号鍵とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成するステップと、
前記暗証番号に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可するステップとを、
有する情報再生方法。
【請求項２０】　情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生装置にて再生するにあたり、
前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出すステップと、
前記記録媒体に設けられた磁気記録領域に記録された暗号鍵を読み出すステップと、
前記記録媒体固有の情報と前記暗号鍵と前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成するステップと、
前記暗証番号に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可するステップとを、
有する情報再生方法。
【請求項２１】　情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生装置にて再生するにあたり、
前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出すステップと、
前記記録媒体に設けられた磁気記録領域に記録された暗号鍵を読み出すステップと、
ユーザが入力する暗証番号を読み取るステップと、
前記記録媒体固有の情報と前記暗号鍵と前記暗証番号とに基づいて前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報を生成するステップと、
前記複数の情報の少なくとも１つを特定する情報に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可するステップとを、
有する情報再生方法。
【請求項２２】　情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生する再生装置であって、
前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出す手段と、
前記記録媒体に設けられた磁気記録領域に記録された暗号鍵を読み出す手段と、
前記記録媒体固有の情報と前記暗号鍵とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成する手段と、
前記暗証番号に基づいて前記記録媒体に記録されている

情報の一部又は全部の再生を許可する手段とを、
有する情報再生装置。
【請求項２３】　情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生する再生装置であって、
前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出す手段と、
前記記録媒体に設けられた磁気記録領域に記録された暗号鍵を読み出す手段と、
前記記録媒体固有の情報と前記暗号鍵と前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成する手段と、
前記暗証番号に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可する手段とを、
有する情報再生装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＤＶＤ（デジタルビデオディスク：デジタルバーサタイルディスク）などの光ディスクに記録されている情報を再生する時点における再生許可の管理に関し、特に不正使用や不正コピー（いわゆる海賊版）を防止することができる光ディスク、暗号鍵生成方法、暗号鍵記録方法、暗号鍵記録装置、情報再生方法、情報再生許可方法、並びに情報再生装置に関する。
【０００２】
【従来の技術】一般に、ＣＤなどのディスクパッケージメディアは、ディスクに記録されている情報が全てディスク所有者に開示されるので、ディスク所有者はディスクを入手した時点でディスクに記録されている全ての情報を利用することができる。したがって、図７の（ｂ）に示すように、ディスクの対価はディスクに記録されている全ての情報に対して設定され、消費者はその対価を支払ってディスクを購入することによりディスク所有者になり、その結果、ディスクに記録されている全ての情報を利用することができる。
【０００３】また、他の流通形態として「超流通システム」が知られている。このシステムはデジタル情報の「所有」ではなく、「利用」に対して対価を支払う考え方であり、図７の（ａ）に示すようにＤＶＤに適用した場合、例えばディスクに記録されている情報（ソフト）を再生するＤＶＤプレーヤにはＩＣカードのコネクタや通信ポートが設けられる。ＩＣカードには再生限度額データがあらかじめ記憶され、このデータは情報の再生毎に減額される。通信ポートは電話回線を介してソフト供給者のコンピュータに接続され、ＤＶＤ再生料金の回収と再生枠の設定を行う。
【０００４】ところで、ディスクそのものは極めて安価に製造することができるので、上記の対価の殆どは、ディスクに記録されている全ての情報の質と量に対するものである。しかしながら、上記のようなシステムでは、利用者にとってディスクに記録されている全ての情報ではなく特定の情報のみを再生したい場合にも、全ての情報に対して対価を支払わなければならないという問題点がある。逆に様々な消費者の要求をあらかじめ想定して、内容を若干変えただけの多種多様なディスクを製造しなくてはならないこともある。
【０００５】これらは消費者にとって不都合なだけでなく、生産者にとってもコストアップや流通の複雑さを生む要因となっている。前述した「超流通システム」は情報に対する対価という点では上記の問題を解決するものであるが、情報の利用状況や利用制限情報を通信ネットワークを介してやりとりするなど、大規模なシステムを要求する。
【０００６】一方、光ディスクを製造した後に、光ディスクの情報記録面の一部に強力なレーザビームなどを照射して、光ディスクの基板や基板上の反射膜を永久変形させ、光ディスク本来の記録密度よりはるかに低密度の情報を記録する方法が、例えば米国特許第５、４００、３１９号などに開示されている。このような技術によりディスク１枚毎に異なる情報を書き込むことができるので、ディスク毎の暗号鍵を設定することができ、ディスクの不正複写や暗号鍵の使い回しといった不正な行為が不可能となる。
【０００７】そこで、本発明者は既に、例えば記録媒体固有のＩＤ、再生したい情報のＩＤ、再生装置のＩＤをあらかじめ設定しておいて、これらの３つのＩＤの少なくとも２つを組み合わせて暗号鍵を生成する手法を開発し、特許出願している（出願日：平成８年１２月３日；　発明の名称：暗号鍵生成方法、光ディスク再生方法及び光ディスク再生装置並びに光ディスク再生許可方法；　整理番号：０４０００６７５；　出願人：日本ビクター株式会社）。この既提案の発明（本願の出願時には未公開）によれば、ユーザは光ディスクを入手後、一度ソフト供給業者に連絡すれば、情報の対価の支払いを条件に、希望する情報の再生を許可する暗号鍵を入手することができる。
【０００８】上記未公開の既提案の発明によれば、記録媒体固有の情報や再生装置固有の情報などを、ソフト供給者側に電話、パソコン通信、郵便など何等かの手段で伝達することにより、ソフト供給者側が暗号鍵を生成してユーザに提供するので、上記超流通システムのようにＩＣカードなどを用いることなく、例えばクレジットカードの番号をソフト供給者側に伝達するだけでよいので、超流通システムより便利で現実的である。
【０００９】
【発明が解決しようとする課題】しかしながら、上記未公開の既提案の発明によれば、記録媒体固有の情報を用

いて暗号鍵を生成するときは、光ディスクＩＤなどを所定のアルゴリズムにて処理して暗号鍵が生成されることから、記録媒体が異なれば、暗号鍵も異なったものとなる。すなわち、複数の記録媒体を用いる場合には、記録媒体毎の暗号鍵が生成されるので、ユーザはこれらの異なる暗号鍵とその対応記録媒体を全て覚えるか、又は記憶装置に保持して、どの暗号鍵がどの記録媒体のものかを管理しておかなくてはならない。かかる管理は記録媒体の数が増加すると、相当面倒であり、ユーザにとって負担となる。

【００１０】したがって、本発明は上記従来の問題点及び上記未公開の既提案の発明における問題点に鑑み、利用者に対する情報の対価とディスク自体を安価にし、ひいては不正コピーを防止することができ、かつユーザによる繁雑な暗号鍵の管理の不要な光ディスク、暗号鍵生成方法、光ディスク再生方法及び光ディスク再生装置並びに光ディスク再生許可方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】本発明は上記目的を達成するために、情報が記録された記録媒体を他の記録媒体から識別する記録媒体固有の情報を記録媒体から読み出し、記録媒体のユーザが設定する任意の暗証番号を読み取り、記録媒体固有の情報と暗証番号とを用いて、所定のアルゴリズムにて演算処理し、記録媒体から情報を読み出すための暗号鍵を生成しておき、ユーザが情報を読み出したいときは、この時点で入力された暗証番号と先に生成された暗号鍵に基づいて記録媒体に記録されている情報の一部又は全部の再生を許可するようにしている。また本発明の他の態様によれば、記録媒体固有の情報と暗証番号に加えて、記録媒体に記録されている複数の情報の少なくとも１つを特定する情報をも用いて所定のアルゴリズムにて演算処理し、記録媒体から情報を読み出すための暗号鍵を生成するようにしてもよい。また、上記生成された暗号鍵を記録媒体の所定の記録領域に記録しておくことは本発明の好ましい態様である。この所定の記録領域として記録媒体固有の情報が記録されている領域に連続又は隣接する領域を用いることは本発明の好ましい態様である。また、この所定の記録領域として記録媒体に設けられた磁気記録領域を用いることは本発明の好ましい態様である。

【００１２】すなわち本発明によれば、情報が記録された光ディスクを他の光ディスクから識別する前記光ディスク固有の情報が光記録された第１領域と、前記光ディスク固有の情報と任意の暗証番号と、又はこれらに加えて、前記光ディスクに記録されている複数の情報の少なくとも１つを特定する情報とを用いて、所定のアルゴリズムにて演算処理し、前記光ディスクから情報を読み出すために生成された暗号鍵を光記録により追記するための領域であって、前記第１領域の記録フォーマットと同一フォーマットであり、かつ前記第１領域と連続又は隣接する第２領域とを、有する光ディスクが提供される。

【００１３】また本発明によれば、情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出すステップと、前記記録媒体のユーザが設定する任意の暗証番号を読み取るステップと、前記記録媒体固有の情報と前記暗証番号とを用いて、所定のアルゴリズムにて演算処理し、前記記録媒体から情報を読み出すための暗号鍵を生成するステップとを、有する暗号鍵生成方法が提供される。

【００１４】また本発明によれば、情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出すステップと、前記記録媒体のユーザが設定する任意の暗証番号を読み取るステップと、前記ユーザが設定する前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報を読み取るステップと、前記記録媒体固有の情報と前記暗証番号と前記複数の情報の少なくとも１つを特定する情報とを用いて、所定のアルゴリズムにて演算処理し、前記記録媒体から情報を読み出すための暗号鍵を生成するステップとを、有する暗号鍵生成方法が提供される。

【００１５】また本発明によれば、情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出すステップと、前記記録媒体のユーザが設定する任意の暗証番号を読み取るステップと、前記記録媒体固有の情報と前記暗証番号とを用いて、所定のアルゴリズムにて演算処理し、前記記録媒体の情報を読み出すための暗号鍵を生成するステップと、前記暗号鍵を前記記録媒体固有の情報が記録されている領域と連続又は隣接する領域に追記するステップとを、有する暗号鍵記録方法が提供される。

【００１６】また本発明によれば、情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出すステップと、前記記録媒体のユーザが設定する任意の暗証番号を読み取るステップと、前記ユーザが設定する前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報を読み取るステップと、前記記録媒体固有の情報と前記暗証番号と前記複数の情報の少なくとも１つを特定する情報とを用いて、所定のアルゴリズムにて演算処理し、前記記録媒体の情報を読み出すための暗号鍵を生成するステップと、前記暗号鍵を前記記録媒体固有の情報が記録されている領域と連続又は隣接する領域に追記するステップとを、有する暗号鍵記録方法が提供される。

【００１７】また本発明によれば、情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出す手段と、前記記録媒体のユーザが設定する任意の暗証番号を読み取る手段と、前記記録媒体固有の情報と前記暗証番号とを所定の暗号鍵生成装置に送信する手段と、前記暗号鍵生成装置から

暗号鍵を受信する手段と、前記暗号鍵を前記記録媒体固有の情報が記録されている領域と連続又は隣接する領域に追記する手段とを、有する暗号鍵記録装置が提供される。

【００１８】また本発明によれば、情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出す手段と、前記記録媒体のユーザが設定する任意の暗証番号を読み取る手段と、前記ユーザが設定する前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報を読み取る手段と、前記記録媒体固有の情報と前記暗証番号と前記複数の情報の少なくとも１つを特定する情報を所定の暗号鍵生成装置に送信する手段と、前記暗号鍵生成装置から暗号鍵を受信する手段と、前記暗号鍵を前記記録媒体固有の情報が記録されている領域と連続又は隣接する領域に追記する手段とを、有する暗号鍵記録装置が提供される。

【００１９】また本発明によれば、情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生装置にて再生するにあたり、前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出すステップと、前記記録媒体固有の情報の記録された領域と連続又は隣接する領域に記録された暗号鍵を読み出すステップと、前記記録媒体固有の情報と前記暗号鍵とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成するステップと、前記暗証番号に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可するステップとを、有する情報再生方法が提供される。

【００２０】また本発明によれば、情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生装置にて再生するにあたり、前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出すステップと、前記記録媒体固有の情報の記録された領域と連続又は隣接する領域に記録された暗号鍵を読み出すステップと、前記記録媒体固有の情報と前記暗号鍵と前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成するステップと、前記暗証番号に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可するステップとを、有する情報再生方法が提供される。

【００２１】また本発明によれば、情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生装置にて再生するにあたり、前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出すステップと、前記記録媒体固有の情報の記録された領域と連続又は隣接する領域に記録された暗号鍵を読み出すステップと、ユーザが入力する暗証番号を読み取るステップと、前記記録媒体固有の情報と前記暗号鍵と前記暗証番号とに基づいて前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報を生成するステップと、前記複数の情報の少なくとも１つを特定する情報に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可するステップとを、有する情報再生方法が提供される。

【００２２】また本発明によれば、情報と、他の記録媒体から識別するための前記記録媒体固有の情報とがあらかじめ記録された記録媒体からユーザが情報を再生装置にて再生するにあたり、前記記録媒体の提供者側にて前記ユーザによる情報の再生を許可するか否かを判断する情報再生許可方法であって、前記記録媒体から読み出された前記記録媒体固有の情報と、前記ユーザが入力した暗証番号を前記再生装置側から受信するステップと、前記記録媒体固有の情報と、前記暗証番号と、又はこれらに加えて、前記光ディスクに記録されている複数の情報の少なくとも１つを特定する情報とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗号鍵を生成するステップと、前記記録媒体に記録されている情報の一部又は全部の再生を許可するために前記暗号鍵を前記再生装置側に送信するステップとを、有する情報再生許可方法が提供される。

【００２３】また本発明によれば、情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生する再生装置であって、前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出す手段と、前記記録媒体固有の情報の記録された領域と連続又は隣接する領域に記録された暗号鍵を読み出す手段と、前記記録媒体固有の情報と前記暗号鍵とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成する手段と、前記暗証番号に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可する手段とを、有する情報再生装置が提供される。

【００２４】また本発明によれば、情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生する再生装置であって、前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出す手段と、前記記録媒体固有の情報の記録された領域と連続又は隣接する領域に記録された暗号鍵を読み出す手段と、前記記録媒体固有の情報と前記暗号鍵と前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成する手段と、前記暗証番号に基づいて前記記録媒体に記録されている

情報の一部又は全部の再生を許可する手段とを、有する情報再生装置が提供される。

【００２５】また本発明によれば、情報が記録された光ディスクを他の光ディスクから識別する前記光ディスク固有の情報が光記録された領域と、前記光ディスク固有の情報と任意の暗証番号と、又はこれらに加えて、前記光ディスクに記録されている複数の情報の少なくとも１つを特定する情報とを用いて、所定のアルゴリズムにて演算処理し、前記光ディスクから情報を読み出すために生成された暗号鍵を磁気記録する領域とを、有する光ディスクが提供される。

【００２６】また本発明によれば、情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出すステップと、前記記録媒体のユーザが設定する任意の暗証番号を読み取るステップと、前記記録媒体固有の情報と前記暗証番号とを用いて、所定のアルゴリズムにて演算処理し、前記記録媒体の情報を読み出すための暗号鍵を生成するステップと、前記暗号鍵を前記記録媒体に設けられた磁気記録領域に記録するステップとを、有する暗号鍵記録方法が提供される。

【００２７】また本発明によれば、情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出すステップと、前記記録媒体のユーザが設定する任意の暗証番号を読み取るステップと、前記ユーザが設定する前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報を読み取るステップと、前記記録媒体固有の情報と前記暗証番号と前記複数の情報の少なくとも１つを特定する情報とを用いて、所定のアルゴリズムにて演算処理し、前記記録媒体の情報を読み出すための暗号鍵を生成するステップと、前記暗号鍵を前記記録媒体に設けられた磁気記録領域に記録するステップとを、有する暗号鍵記録方法が提供される。

【００２８】また本発明によれば、情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出す手段と、前記記録媒体のユーザが設定する任意の暗証番号を読み取る手段と、前記記録媒体固有の情報と前記暗証番号とを所定の暗号鍵生成装置に送信する手段と、前記暗号鍵生成装置から暗号鍵を受信する手段と、前記暗号鍵を前記記録媒体に設けられた磁気記録領域に記録する手段とを、有する暗号鍵記録装置が提供される。

【００２９】また本発明によれば、情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を前記記録媒体から読み出す手段と、前記記録媒体のユーザが設定する任意の暗証番号を読み取る手段と、前記ユーザが設定する前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報を読み取る手段と、前記記録媒体固有の情報と前記暗証番号と前記複数の情報の少なくとも１つを特定する情報を所定の暗号鍵生成装置に送信する手段と、前記暗号鍵生成装置から暗号鍵を受信する手段と、前記暗号鍵を前記記録媒体に設けられた磁気記録領域に記録する手段とを、有する暗号鍵記録装置が提供される。

【００３０】また本発明によれば、情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生装置にて再生するにあたり、前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出すステップと、前記記録媒体に設けられた磁気記録領域に記録された暗号鍵を読み出すステップと、前記記録媒体固有の情報と前記暗号鍵とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成するステップと、前記暗証番号に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可するステップとを、有する情報再生方法が提供される。

【００３１】また本発明によれば、情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生装置にて再生するにあたり、前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出すステップと、前記記録媒体に設けられた磁気記録領域に記録された暗号鍵を読み出すステップと、前記記録媒体固有の情報と前記暗号鍵と前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成するステップと、前記暗証番号に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可するステップとを、有する情報再生方法が提供される。

【００３２】また本発明によれば、情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生装置にて再生するにあたり、前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出すステップと、前記記録媒体に設けられた磁気記録領域に記録された暗号鍵を読み出すステップと、ユーザが入力する暗証番号を読み取るステップと、前記記録媒体固有の情報と前記暗号鍵と前記暗証番号とに基づいて前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報を生成するステップと、前記複数の情報の少なくとも１つを特定する情報に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可するステップとを、有する情報再生方法が提供される。

【００３３】また本発明によれば、情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生する再生装置であって、前記情報が記録された記録媒体を他の記録媒体から識別する前記

記録媒体固有の情報を、前記記録媒体から読み出す手段と、前記記録媒体に設けられた磁気記録領域に記録された暗号鍵を読み出す手段と、前記記録媒体固有の情報と前記暗号鍵とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成する手段と、前記暗証番号に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可する手段とを、有する情報再生装置が提供される。

【００３４】また本発明によれば、情報と、他の記録媒体から識別するための情報とがあらかじめ記録された記録媒体から情報を再生する再生装置であって、前記情報が記録された記録媒体を他の記録媒体から識別する前記記録媒体固有の情報を、前記記録媒体から読み出す手段と、前記記録媒体に設けられた磁気記録領域に記録された暗号鍵を読み出す手段と、前記記録媒体固有の情報と前記暗号鍵と前記記録媒体に記録されている複数の情報の少なくとも１つを特定する情報とに基づいて前記記録媒体に記録された情報の一部又は全部を再生するための暗証番号を生成する手段と、前記暗証番号に基づいて前記記録媒体に記録されている情報の一部又は全部の再生を許可する手段とを、有する情報再生装置が提供される。

【００３５】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。図１は本発明に係る暗号鍵生成方法、光ディスク再生方法及び光ディスク再生装置並びに光ディスク再生許可方法の一実施形態を示す説明図、図２は図１の光ディスク再生装置における処理を説明するためのフローチャートであり、図３は図１のソフトハウスにおける処理を説明するためのフローチャートである。

【００３６】図１は一例として、ゲームソフトが記録された光ディスク１をディスク再生装置２により再生し、また、再生の対価をソフトウエア（以下ソフト）の提供者であるソフトハウス３がディスク再生装置２のユーザから徴収するシステムを示し、このシステムではディスク１は例えば雑誌などの付録として無料又はごく安価にユーザに提供される（図示 ①）。ディスク１の情報エリアには例えば５０個のゲームソフトとディスク１を他のディスクから識別する固有の情報（以下、ディスクＩＤ）が記録されている。また、個々のゲームソフト毎、あるいはすべてのゲームソフトを包含する形で固有の情報（以下、タイトルキー）が設定され、この実施形態ではこのタイトルキーとソフトの通し番号が１対１で対応している。なお、代わりにタイトルキーと例えばソフトのファイル名などを対応させてもよい。後述するように、ディスク提供者であるソフトハウス３とユーザ側であるディスク再生装置２は通信回線などを介して相互に通信可能であり、それぞれ図示省略のＣＰＵ（中央演算処理装置）やインターフェースを有しているものとする。

【００３７】また、ディスク１の例えばセクタヘッダには、暗号鍵が入力されなくても再生を許可するエリア（例えばソフト毎の第１シーン）のアドレス情報と、暗号鍵の入力を条件として再生を許可するエリア（ソフト本体）のアドレス情報が記録されている。そして、ディスク再生装置２はディスク１を再生する場合、ソフト毎に例えばソフトの第１シーンが再生可能であるが、そのソフトのその後は暗号鍵が入力されないと再生することができないように構成されている。

【００３８】また、ディスクＩＤの記録方法としては、例えば米国特許５，４００，３１９号に示されるように、ディスク１の表面に記録密度よりはるかに低密度の情報を記録した後に、ディスクＩＤを示す２進データ「１」、「０」に応じて変調された強力なレーザ光を照射してデータ「１」の位置ではディスク１の反射膜を永久変形させることにより、「反射有り＝１」、「反射無し＝０」のようにバーコードとして記録することができる。この実施形態では、ディスクＩＤの一例としてＤＶＤにおいて用いられているＢＣＡ番号が記録され、このＢＣＡ番号はディスク再生装置２により読み取られて例えば１０進数字で表示される。

【００３９】ＢＣＡは光ディスクの光記録部分の最内周部分の複数のトラックにまたがって、ＹＡＧレーザビームなどの強力な光ビームにてバーコードを形成した領域、及びバーコードを追記できるような領域であり、バーストカッティングエリアともいう。ＢＣＡ番号とは、ＢＣＡにバーコードとして記録された情報の中で、１枚１枚のディスク固有の情報をいう。なお、ＢＣＡに限らず、ディスクに磁気記録領域など他の記録方式による部分を設け、これを専用のヘッドで読み出すようにしてもよい。

【００４０】ディスク再生装置２には、ユーザが暗証番号を入力するためのテンキーが設けられている。この暗証番号と、前述したＢＣＡ番号と、光ディスク１に記録されている複数の情報の少なくとも１つを特定する情報としてのタイトルキー暗号鍵を生成するためのコードとして用いられている。

【００４１】ディスク再生装置２ではディスク１がセットされると、暗号鍵がなくても再生を許可するエリアのみを再生して表示する。これにより、ユーザは再生したい所望のソフトの概要あるいは冒頭部分を知ることができるが、そのソフトの暗号鍵はユーザにとって不明である。ここで、一例として所望のソフト番号「０１」のタイトルキーを「０８００１」とする。

【００４２】先ず、ディスク再生装置２やユーザは、ソフトハウス３に対して例えばモデムやＰＢ信号と電話回線やＩＳＤＮ回線を介して

・ディスク１のＢＣＡ番号（例えば「００１２３」）

と、

・ユーザが任意に設定する暗証番号（例えば「０１０１０」）と
・対価支払いのためのクレジットカード番号と
・所望のソフトの番号「０１」

を知らせる（図示②）。この場合、再生を許可する暗号鍵は例えば、

【００４３】

【数１】

暗号鍵＝「タイトルキー」－「ＢＣＡ番号」－「暗証番号」
＝０８００１－００１２３－０１０１０
＝０６８６８

【００４４】とする。次いで、ソフトハウス３はディスク１のソフトの番号「０１」を再生する対価を支払う条件で、例えばモデムなどを用いてこの暗号鍵をディスク再生装置２に送る（図示 ③）。

【００４５】図２～６はディスク再生装置２及びソフトハウス３における処理手順を示したもので、図１のソフトハウス３との通信を介して暗号鍵が生成され、それを用いて暗証番号が生成される様子が示されている。まず図２はディスク再生装置２において、ソフトハウス３に所定の各情報を送信する手順を示している。まず、ステップＳ１でディスクＩＤを読み出し、ステップＳ２でユーザに対して暗証番号の入力を要求する。ユーザは任意の暗証番号を決めて、ディスク再生装置３の図示省略のテンキーを用いてこれを入力する。ステップＳ３で暗証番号の入力を確認すると、ステップＳ４で再生したいソフトの番号の入力を要求し、ステップＳ５でその入力を確認する。次いでステップＳ６でクレジットカード番号の入力を要求し、ステップＳ７でその入力を確認する。これらの各情報が入力されると、ステップＳ８で各情報をソフトハウス３に送信し、送信完了を確認して送信処理を終了する。

【００４６】図３はソフトハウス３側における処理手順を示すフローチャートである。ソフトハウス３ではステップＳ１１でユーザ、すなわちディスク再生装置２からの情報を受信したことを確認すると、ステップＳ１２で上記手法で暗号鍵を生成し、次いで生成された暗号鍵をステップＳ１３でユーザに送信する。送信完了がステップＳ１４で確認されると、ステップＳ１５で受信されたユーザのクレジットカード番号により、所定の課金処理を行い、ソフトハウス３側の処理を終了する。

【００４７】図４はディスク再生装置２において、ソフトハウス３から送信された暗号鍵を光ディスク１に書き込む手順を示している。すなわち、ステップＳ１８にて暗号鍵の受信を確認すると、ステップＳ１９でディスクの所定領域に受信した暗号鍵を書き込み、書き込みの終了をステップＳ２０で確認して処理を終了する。よってディスク再生装置は暗号鍵追記装置としても動作することとなる。ディスクの所定領域としては、ＢＣＡの追記領域を用いることができる。この、ＢＣＡの追記領域とは、ディスクＩＤがＢＣＡ番号として記録されているＢＣＡの一部で、ＢＣＡ番号の記録されている領域に連続又は隣接する領域である。連続する領域としては、ＢＣＡ中のディスクＩＤの記録領域の円周方向の連続部分のバーコード追記可能領域があり、また隣接する領域としては同様にディスクの半径方向に隣接するバーコード追記可能部分がある。

【００４８】次に図５により、所望の情報を光ディスク１から再生するための手順について説明する。図５はディスク再生装置２における再生許可の処理手順を示すフローチャートである。いま、光ディスク１には先に説明した図４の処理により、ソフトハウスで生成した暗号鍵が記録されているものとする。ステップＳ２１でディスクＩＤを読み出し、次いでステップＳ２２で暗号鍵を読み出す。これらの情報はいずれもＢＣＡに記録されていて、バーコードとして読み出される。ステップＳ２３で暗号鍵の存在が確認されると、ステップＳ２４でタイトルキーを検出する。タイトルキーの検出はユーザが入力する再生したいソフトの番号に１対１で対応する番号を見出すことであり、例えば、ソフト番号００１に対応するタイトルキー０８００１が検出される。

【００４９】ステップＳ２５では、ステップＳ２１、Ｓ２２で読み出されたディスクＩＤ、暗号鍵とステップＳ２４で検出されたタイトルキーを用いて次式に示すように暗証番号を算出する。

【００５０】

【数２】

暗証番号＝「タイトルキー」－「ＢＣＡ番号」－「暗号鍵」
＝０８００１－００１２３－０６８６８
＝０１０１０

【００５１】こうして算出された暗証番号を算出暗証番号という。次に、ステップＳ２６でユーザに対して暗証番号の入力を要求する。この暗証番号を入力暗証番号という。ステップＳ２７で入力暗証番号が入力されたかを判断し、入力されるとステップＳ２８で入力暗証番号が算出暗証番号と一致するか否かを判断する。一致するとステップＳ２９で該当タイトルの再生を許可するためにタイトルキー「０８００１」に対応するディスク１のソフトの番号「０１」の再生を許可し、一致しないとき並びにステップＳ２３で暗号鍵が検出されなかったときはステップＳ３０でソフトの再生が実行できないよう再生を不許可とする。

【００５２】上記実施例では暗証番号を算出して、ユーザが入力した暗証番号と一致するか否かを判断している

が、これに限らず、入力された暗証番号を用いてタイトルキーを算出するようにしてもよい。図６は、タイトルキーを算出してソフトの再生を許可するか否かを判断する場合の手順を示すフローチャートである。図５と同じステップは同一のステップ番号で示し、その説明を省略する。図６のフローチャートにおいて、ステップＳ２３で暗号鍵の存在が確認されると、ステップＳ２６でユーザに対して暗証番号の入力を要求し、その入力がステップＳ２７で確認されると、ステップＳ３１で次式に示すようにタイトルキーを算出する。

【００５３】

【数３】

タイトルキー＝「ＢＣＡ番号」＋「暗号鍵」＋「暗証番号」
＝００１２３＋０６８６８＋０１０１０
＝０８００１

【００５４】次いでステップＳ３２で算出されたタイトルキーに対応するタイトルが光ディスク１に存在するか否かを判断する。存在するときは、ステップＳ２９で該当タイトルの再生を許可する。一方、該当タイトルが存在しないときと、ステップＳ２３で暗号鍵が検出されなかったときはステップＳ３０で再生を不許可とする。

【００５５】すなわち、ディスク再生装置２のユーザは、ディスク１を保持していてもソフトハウス３に対して対価を支払う必要がない情報については自由に再生することができるが、その後の情報については対価をソフトハウス３に支払ってソフトハウス３から暗号鍵を知得しない限り再生することができない。

【００５６】上記実施例において、ディスクＩＤは００１２３としたが、いま別のディスクから情報を再生する場合について検討する。この別のディスクのディスクＩＤを００１５０とする。先に図３で説明したように、ソフトハウス３では暗号鍵を生成するが、ディスクＩＤが００１５０、暗証番号が１０１０、タイトルキーが８００１とすると、暗号鍵は０６８４１となる。このディスクにはこの新しい暗号鍵が図４の処理により記録される。この暗号鍵により暗証番号又はタイトルキーが生成される。したがって、このディスクから情報を再生する際には、先に説明したディスクＩＤが００１２３のディスクのときと同一の暗証番号０１０１０を入力することにより、所望のソフトを再生することができる。

【００５７】上記実施例では、生成された暗号鍵はＢＣＡの追記部分、すなわちディスクＩＤの記録領域と連続又は隣接する領域に記録されるものとして説明したが、暗号鍵はディスクの光記録領域よりさらに内周の、いわゆるラベル部分に設けられた磁気記録領域に磁気記録により記録することもできる。

【００５８】上記の暗号鍵の生成方法は説明を簡略化するためのものであり、実際にはセキュリティを高めるために複雑な暗号生成論理（アルゴリズム）に基づいて生成される。また、ディスクＩＤと暗証番号の桁数も一例であり、例えば暗証番号に数字ではなくて、アルファベットの文字や記号を用いたり、数字と文字の組み合わせとして、桁数も変更してもよい。暗証番号の桁数は多い程不正使用に強いと言えるが、あまり桁数が多いと記憶や、入力が面倒となるので１ないし３０バイトの範囲内が望まれる。

【００５９】また、上記実施の形態ではタイトルキーをディスクに記録された複数の情報の１つを特定する情報として説明しているが、ディスク全体の情報に対する再生許可情報として扱うこともできる。さらに、タイトルキーをディスクに記録された複数の情報の組み合わせを特定する情報として取り扱うこともできる。例えば、タイトルキーとして４バイト＝３２ビットを割り当てると、各ビットに対応して３２種類の情報を特定することができるので、複数の情報に対する再生許可情報としてタイトルキーを扱うことができる。

【００６０】ディスクＩＤは必ずしもＢＣＡ番号そのものではなくてもよく、ＢＣＡ番号の情報が正確に含まれるように再生装置内でエンコードされていてもよい。この場合はデコードの機能も再生装置は持っている必要があるが、暗号鍵の秘匿性向上に有効な手法である。なお、上記実施例では、ディスク再生装置が暗号鍵追記装置としても動作するものとして説明したが、ディスク再生装置にかかる機能をもたせるのではなく、暗号鍵追記装置を別個に設け、その暗号鍵追記装置に受信した暗号鍵を入力してディスクＩＤ領域にバーコードとして、又は磁気記録領域に磁気記録により追記するようにしてもよい。

【００６１】また、ソフト供給元から返信される暗号鍵は、必ずしも暗号鍵そのものではなくてもよく、ユーザにわからない形にエンコードされていてもよい。その場合は暗号鍵記録時又はディスク再生の暗号鍵読み出し時にこのデータがデコードされて、タイトルキーが生成される。ディスクＩＤ記録領域に追記された暗号鍵情報は、ディスクＩＤ記録領域に未記録領域が残っている限り追記可能であり、擬似的に書換えができるので、ユーザが設定した暗証番号が仮に都合の悪いものになった場合、改めてソフト供給者にその旨連絡すれば、暗証番号は変更可能である。また、磁気記録領域を備えたディスクにおいて、磁気記録領域に記録された暗号鍵情報は書換え可能であるので、ユーザが設定した暗証番号が仮に都合の悪いものになった場合、改めてソフト供給者にその旨連絡すれば暗証番号は変更可能である。同様にして、ディスクに含まれる情報が複数有り、利用したい情報を後から追加したい場合には、新しい暗号鍵を追記していくか、古い暗号鍵情報を含む形で新しい暗号鍵に書き換えればよい。この際、以前と同じ暗証番号が利用で

きるので便利である。

【００６２】また、複数の情報に対して異なる暗証番号を設定することもでき、任意のタイトルの組み合わせで再生制限をかけることもできる。また、記録媒体に記録された複数の情報のうち少なくとも一つを特定する情報は、記録媒体に記録された複数の情報のうち少なくとも一つの再生を許可する情報と同義であり、再生制限情報そのものである。したがって、実施例中タイトルキーとされている情報は再生制限情報としてもよく、タイトルが一つ（情報が一つ）の場合には記録媒体の再生許可情報に相当する。

【００６３】したがって、このような方法によれば、利用者にとってディスク１に記録されている全ての情報ではなく特定の情報のみを再生したい場合にその情報に対してのみ対価を支払えばよいので、対価が安価になるとともに不正再生を防止することができる。また、これにより多数の情報が記録されたディスク１を大量生産することができるので、ディスク１を安価にすることができ、ディスク１が安価であれば海賊版も横行しない。

【００６４】

【発明の効果】以上説明したように本発明によれば、ユーザが任意に設定した暗証番号を用いて暗号鍵が自動的に生成されるので、ユーザによる繁雑な暗号鍵の管理が不要であり、複数のディスクに共通な暗証番号を用いて情報の選択的再生許可を実現できる。よって、ユーザの利便性が図られるとともに情報の対価とディスク自体を安価にし、また、不正コピーを防止することができる。

【００６５】本発明の効果を整理すると、情報そのものに対して課金するため、ディスクは安価に配布でき、消費者は自分が必要とする情報部分にのみ対価を支払えばよいので無駄な出費がなく、ディスクは極めて安価に流通するので、海賊版が成立せず、ユーザから暗号鍵配布の依頼があった時点でディスクの流通先が確実に解るので、ユーザ管理が確実にでき、不正コピーディスクの把握も容易であり、安価なディスクをとりあえず入手して各ソフトの非暗号部分で内容を確認してから情報の購入ができるので、流通が活発になるといった基本的利点に加え、暗証番号はユーザが任意に設定できるので、全ての所有ディスクに対して同じ番号を設定することもでき、ディスクごとに暗証番号を覚えておく必要がなく、ソフト供給者から伝えられる暗号鍵はそのディスクに対してのみ有効なので、そのほかのディスクに対して悪用されることはなく、一度、あるディスク、あるソフト供給者に対して登録をしておけば、暗証番号を変えたい場合にはもう一度ソフト供給者に連絡すればよいので、いつでも暗証番号は変更可能であり、複数の情報が含まれるディスクに対して、利用したい情報の追加が可能であり、その際も同じ暗証番号を使え、もちろん変えることも可能であり、さらに複数の情報に対して異なる暗証番号を設定することもできるという効果がある。

【図面の簡単な説明】

【図１】本発明に係る暗号鍵生成方法、光ディスク再生方法及び光ディスク再生装置並びに光ディスク再生許可方法の一実施形態を示す説明図である。

【図２】図１の光ディスク再生装置における情報の送信処理を説明するためのフローチャートである。

【図３】図１のソフトハウスにおける暗号鍵生成とその送信処理を説明するためのフローチャートである。

【図４】図１の光ディスク再生装置における暗号鍵の受信とそのディスクへの書き込み処理を説明するためのフローチャートである。

【図５】図１の光ディスク再生装置における再生許可・禁止の処理の一例を説明するためのフローチャートである。

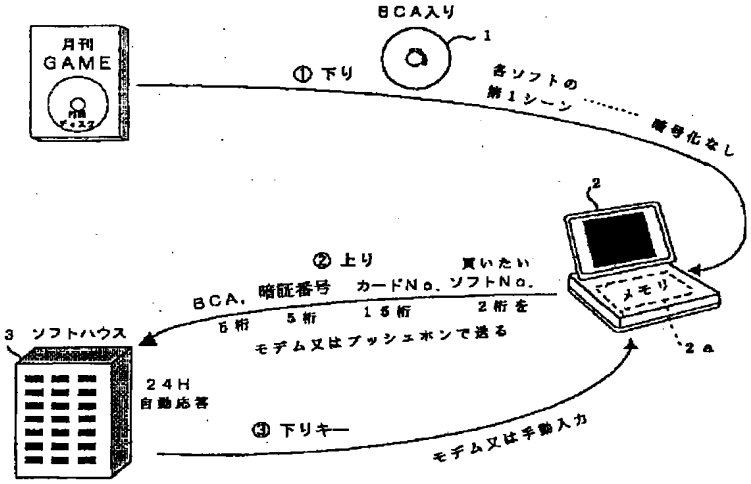
【図６】図１の光ディスク再生装置における再生許可・禁止の処理の他の例を説明するためのフローチャートである。

【図７】ソフトハウスとユーザ間の従来のソフト提供形態を模式的に示す図である。

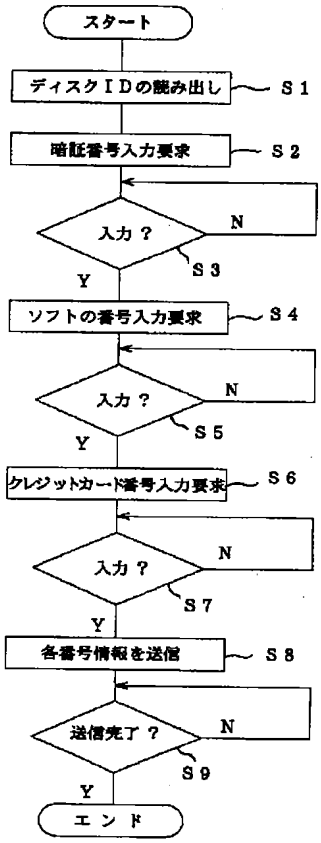
【符号の説明】

１　光ディスク
２　光ディスク再生装置
２ａ　メモリ
３　ソフトハウス

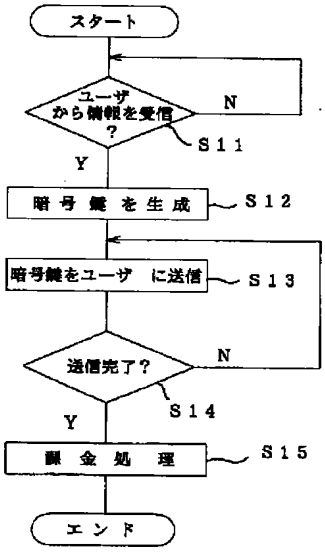
【図１】


月刊
GAME
BCA入り
1
① 下り
各ソフトの
第１シーン
暗号化なし
2
② 上り
買いたい
BCA，暗証番号　カードNo．ソフトNo．
５桁　５桁　１５桁　２桁を
モデム又はプッシュホンで送る
メモリ
2a
3　ソフトハウス
２４Ｈ
自動応答
③ 下りキー
モデム又は手動入力

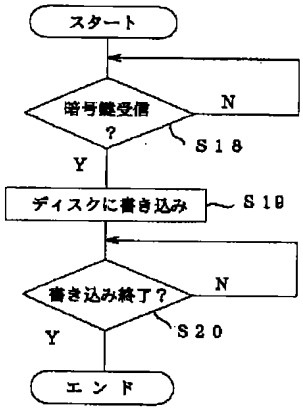
【図２】


スタート
ディスクＩＤの読み出し
S１
暗証番号入力要求
S２
入力？
N
S３
Y
ソフトの番号入力要求
S４
入力？
N
S５
Y
クレジットカード番号入力要求
S６
入力？
N
S７
Y
各番号情報を送信
S８
送信完了？
N
S９
Y
エンド

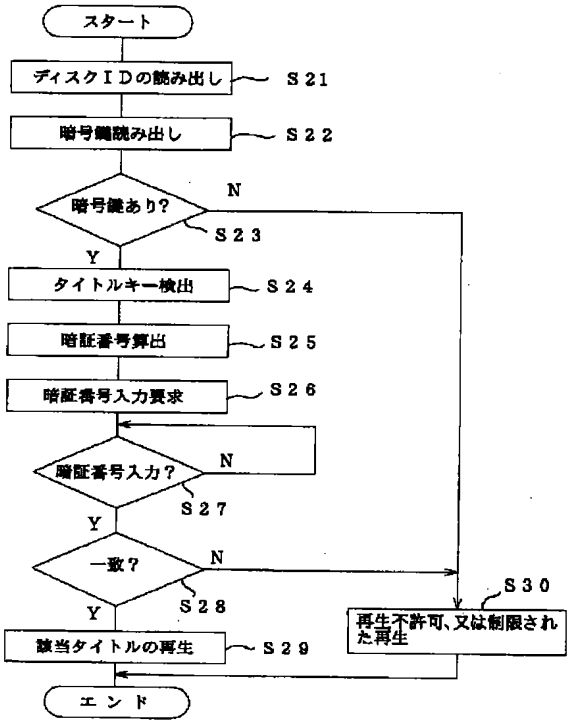
【図３】


スタート
ユーザ
から情報を受信
？
N
S１１
Y
暗号鍵を生成
S１２
暗号鍵をユーザ　に送信
S１３
送信完了？
N
S１４
Y
課金処理
S１５
エンド

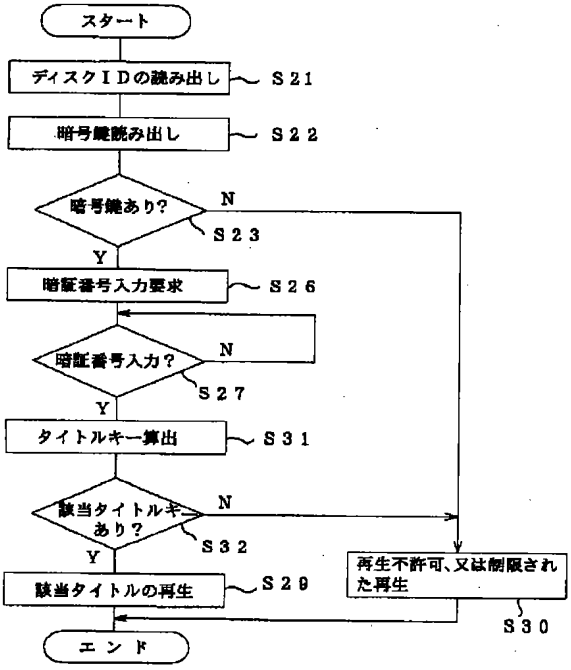
【図４】


スタート
暗号鍵受信
？
N
S１８
Y
ディスクに書き込み
S１９
書き込み終了？
N
S２０
Y
エンド

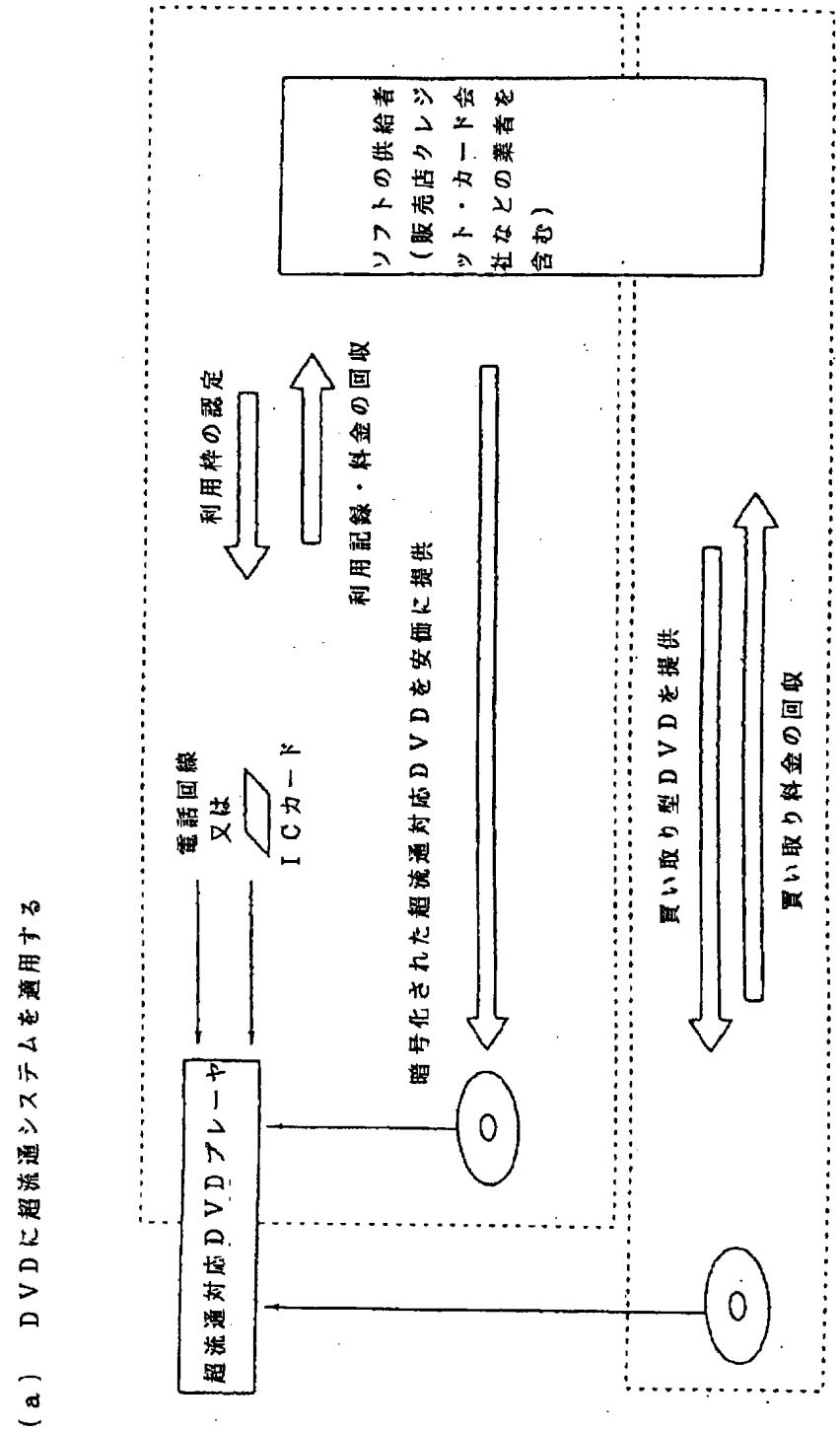
【図５】


スタート
ディスクＩＤの読み出し
S21
暗号鍵読み出し
S22
暗号鍵あり?
N
S23
Y
タイトルキー検出
S24
暗証番号算出
S25
暗証番号入力要求
S26
暗証番号入力?
N
S27
Y
一致?
N
S28
Y
該当タイトルの再生
S29
再生不許可、又は制限された再生
S30
エンド

【図６】


スタート
ディスクＩＤの読み出し
S21
暗号鍵読み出し
S22
暗号鍵あり?
N
S23
Y
暗証番号入力要求
S26
暗証番号入力?
N
S27
Y
タイトルキー算出
S31
該当タイトルキーあり?
N
S32
Y
該当タイトルの再生
S29
再生不許可、又は制限された再生
S30
エンド

【図７】



（ａ）　ＤＶＤに超流通システムを適用する

（ｂ）　通常の販売システム